APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **RISK MANAGEMENT CLEARINGHOUSE**

APPLICANT: **David Lawrence**

RISK MANAGEMENT CLEARINGHOUSE

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of a prior application entitled "Automated Global Risk Management" filed March 20, 2001, bearing the Serial No. 09/812,627, the contents of which are relied upon and incorporated by reference.

BACKGROUND

This invention relates generally to a method and system for facilitating the identification, investigation, assessment and management of legal, regulatory financial and reputational risks ("Risks"). In particular, the present invention relates to a computerized system and method for banks and non-bank financial institutions to access information compiled on a worldwide basis and relate such information to a transaction at hand, wherein the information is conducive to quantifying and managing financial, legal, regulatory and reputational risk associated with the transaction.

Bank and non-bank financial institutions, including: investment banks; merchant banks; commercial banks; securities firms, including broker dealers securities and commodities trading firms; asset management companies, hedge funds, mutual funds, credit rating funds, securities exchanges and bourses, institutional and individual investors, law firms, accounting firms, auditing firms and other entities, hereinafter collectively referred to as "Financial Institutions," typically have few resources available to them to assist in the identification of present or potential risks associated with business transactions. Risk can be multifaceted and far reaching. Generally, personnel do not have available a mechanism to provide real time assistance to assess a risk factor or otherwise qualitatively manage risk. In the event of problems, it is often difficult to quantify to regulatory bodies, shareholders, newspapers and other interested parties, the diligence exercised by the financial institution to properly identify and respond to risk factors. Absent a means to quantify good business practices and diligent efforts to contain risk, a financial institution may appear to be negligent in some respect.

Risk associated with maintaining an investment account can include factors associated with financial risk, legal risk, regulatory risk and reputational risk. Financial risk includes factors indicative of monetary costs that the financial institution may be exposed to as a result of performing a particular transaction. Monetary costs can be related to fines, forfeitures, costs to defend an adverse position, lost revenue, or other related potential sources of expense. Regulatory risk includes factors that may cause the financial institution to be in violation of rules put forth by a regulatory agency such as the Securities and Exchange Commission (SEC). Reputational risk relates to harm that a financial institution may suffer regarding its professional standing in the industry. A financial institution can suffer from being associated with a situation that may be interpreted as contrary to an image of honesty and forthrightness.

Risk associated with an account involved in international transactions can be greatly increased due to the difficulty in gathering and accessing pertinent data on a basis timely to managing risk associated with the transaction. As part of due diligence associated with performing financial, it is imperative for a financial institution to "know their customer" including whether a customer is contained on a list of restricted entities published by the Office of Foreign Access Control (OFAC), the Treasury Office or other government or industry organization.

However, financial institutions do not have available a mechanism which can provide real time assistance to assess a risk factor associated with an international transaction, or otherwise qualitatively manage such risk. In the event of investment problems, it is often difficult to quantify to regulatory bodies, shareholders, newspapers and/or other interested parties, the diligence exercised by the financial institution to properly identify and respond to risk factors. Absent a means to quantify good business practices and diligent efforts to contain risk, a financial institution may appear to be negligent in some respect.

What is needed is a method and system to draw upon information gathered globally and utilize the information to assist with risk management and due diligence related to financial transactions. A new method and system should anticipate offering guidance to personnel who interact with clients and help the personnel identify high risk situations. In addition, it should be

situated to convey risk information to a compliance department and be able to demonstrate to regulators that a financial institution has met standards relating to risk containment.

SUMMARY

Accordingly, the present invention provides a risk management method and system for facilitating analysis and quantification of risk associated with a financial transaction. An automated risk management clearinghouse (RMC) system maintains a database relating risk variables including world events government advisories, and other information sources with potential risk for a financial institution. The RMC system can be accessed directly or tied into front end or backend systems to automatically monitor transactions. A rating system is used to assess risk based upon criteria such as risk advisories, historical data, interpretation of world events or other variables that can effect risk.

Information generated by an RMC system can be utilized to generate a risk quotient or other rating based upon a weighted algorithm applied to the criteria, wherein the risk quotient is indicative of risk associated with a transaction or an account. The quotient can be monitored on a periodic basis, during the course of a transaction, upon account opening or on demand. Actions commensurate with a risk quotient can be presented to a financial institution to help the institution properly manage risk associated with a particular entity or transaction.

A log or other stored history can be created such that utilization of the system can mitigate adverse effects relating to a problematic transaction. Mitigation can be accomplished by demonstrating to regulatory bodies, shareholders, news media and other interested parties that corporate governance is being addressed through tangible risk management processes. In summary fashion, the present invention includes a method and system for identifying risks associated with the domestic and global commercial activities of financial firms including, for example, a transaction involving: a financial institution, an insurance company, a credit card issuer, a trading exchange, a government regulator, a law enforcement agency, an investment and/or merchant bank, public and private financing, commodities and securities trading, commercial and consumer lending, asset management, the ratings of corporations and securities, public and private equity investments, public and private fixed income investments, the listing of

companies on securities exchanges and bourses, employee screening and hereinafter collectively referred to as "Financial Transactions."

In another aspect, a computer system for providing risk management relating to financial transactions can include a computer server that is accessible with a network access device or computer system via a communications network or direct link and executable software stored on the server which is executable on demand. The software can be operative with the server to gather or receive information relating to risk factors and formulate a risk quotient or other rating. In addition, where applicable, risk can be aggregated, such as by rating, and transferred.

The present invention includes a computer-implemented method for managing risk related to financial transactions involving international or global exposure. The method includes receiving information relating to specific details of a financial transaction and structuring the information received according to risk quotient criteria. A risk quotient is calculated using the structured information. A suggested action responsive to the risk quotient or the information received can also be generated.

Typically the suggested actions will be directed towards reducing risk relating to a transaction associated with international exposure, although actions can be directed towards law enforcement or other directives also. In one embodiment, the action can include refusing to perform a transaction. Another action may involve notifying an authority, such as a law enforcement agency.

In another aspect, the information received, including specific documentation can be stored, as can a suggested action, and utilized to generate a diligence report. The diligence report can include information received relating to an account and actions taken responsive to the risk quotient.

Still another aspect can include aggregating risk quotients relating to a financial institution to assess a level of identified risk to which the financial institution is exposed. An average risk quotient associated with a transaction can also be calculated.

Other embodiments include a computerized system for managing risk associated with a financial account, computer executable program code residing on a computer-readable medium,

a computer data signal embodied in a digital data stream, or a method of interacting with a network access device. Various features and embodiments are further described in the following figures, drawings and claims.

DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a block diagram that can embody this invention.

Fig. 2 illustrates a network on computer systems that can embody an automated RMC system.

Fig. 3 illustrates a flow of exemplary steps that can be executed by a RMC system.

Fig. 4 illustrates a flow of exemplary steps that can taken by a user of the RMC system.

Fig. 5 illustrates an exemplary graphical user interface useful for gathering information according to the present invention.

Fig. 6 illustrates an exemplary graphical user interface useful for presenting reports related to RMC.

DETAILED DESCRIPTION

The present invention includes a computerized method and system for managing risk associated with financial transactions including those with international exposure. A computerized system gathers and stores information in a database or other data storing structure and relates the information to risk factors pertaining to financial transactions. Documents and sources of information can also be stored. A subscriber, such as a Financial Institution can supply information into the database and also query the database. Queries can be automated and made a part of standard operating procedure for each transaction conducted by the subscriber.

A rating system can be used by a subscriber to assess risk based upon the information received and the risk factors. A rating, such as a risk quotient can be generated to readily indicate a level of risk associated with a particular transaction or account holding entity. The risk quotient can be based upon a weighted algorithm applied to the risk factors. The risk quotient can be made available on a periodic basis, on demand in real time, in response to an

event such as a transaction, or according to some other request. Actions commensurate with a risk level can be presented to assist with proper risk management.

Referring now to Fig. 1 a block diagram of one embodiment of the present invention is illustrated. A Risk Management Clearinghouse(RMC) system 106, receives information which may be related to a financial transaction, or a participant to a financial transaction. Information can be received, for example, from publicly available sources, subscribers, investigation entities, or other sources. The information is constantly updated and related to financial transactions or alert lists in order to facilitate compliance with regulatory requirements.

Public information can be received from a variety of information sources, for example, from formalized lists, such as: a list generated by the Office of Foreign Assets Control (OFAC) 101 including their sanction and embargo list, a list generated by the U.S. Commerce Department 102, a list of international "kingpins" generated by the U.S. White House 103, a list generated by a foreign counterpart to a U.S. entity 104, U.S. regulatory actions 105 or other information source 107 such as a foreign government, US adverse business-related media reports, US state regulatory enforcement actions, international regulatory enforcement actions, international adverse business-related media reports, a list of politically connected individuals and military leaders, a list of U.S. and international organized crime members and affiliates, or a list of recognized high risk countries. Court records or other references relating to fraud, bankruptcy, professional reprimands or a rescission of a right to practice, suspension from professional ranks, disbarment, prison records or other sources of suspect behavior can also be important. Information sources can include various foreign equivalents to those listed above or any other international source.

A subscriber institution 112 can include: a securities broker, retail bank, commercial bank, investment and merchant bank, private equity firm, asset management company, mutual fund company, hedge fund firm, insurance company, credit card issuer, retail and commercial financier, securities exchange, other Regulator, money transfer agency, or other entities. Information supplied by a subscriber may be information gathered according to normal course of dealings with a particular entity. Information received from a subscriber may be subject to applicable law including privacy laws, wherein safeguards can be put in place to prevent such

information from being made available to other entities. In addition, a financial institution, or other subscriber may discover or suspect that a person or entity is involved in some fraudulent or otherwise illegal activity and report this information to the RMC system 106.

A decision by a financial institution concerning whether to pursue a financial transaction can be dependent upon many factors. A multitude and diversity of risks related to the factors may need to be identified and evaluated. In addition, the weight and commercial implications of the factors and associated risks can be interrelated. The present invention can provide a consistent and uniform method for business, legal, compliance, credit and other personnel of financial institutions to identify and assess risks associated with a transaction. A RMC system 106 allows investment activity risks to be identified, correlated and quantified by financial institutions thereby assessing legal, regulatory, financial and reputational exposure.

Financial institutions are often closely regulated. As a result financial institutions are exposed to significant risks from their obligations of compliance with the law and to prevent, detect and, at times, report potential violations of laws, regulations and industry rules ("laws"). These risks include, but are not limited to, the duty to disclose material information, and to prevent and possibly report: fraud, money laundering, foreign corrupt practices, bribery, embargoes and sanctions. Through a series of structured questions and weighting of information received as answers, financial institutions can structure a risk exposure and receive suggested responses to a specific risk scenario.

A financial institution can integrate a RMC system 106 as part of legal and regulatory oversight for various due diligence and "know your customer" obligations imposed by regulatory authorities. The RMC system 106 can facilitate detection and reporting of potential violations of law as well as address the "suitability" of a financial transaction and/or the assessment of sophistication of a customer. Similarly, the RMC system 106 can support a financial institution's effort to meet requirements regarding the maintenance of accurate books and records relating to their financial transactions and affirmative duty to disclose material issues affecting an investor's decisions.

The RMC system 106 provides a risk management database which allows a subscriber to screen the names of any or all transactors, including current and/or prospective account holders

and/or wire transfer receipt/payment parties through various due diligence checks on a very low cost and timely basis.

An institution that may implement, or make use of the present invention can include an investment bank, a merchant bank, a commercial bank, a security firm, an asset management company, a hedge fund, a mutual fund, a credit rating agency, a security exchange and bourse, an institutional or individual investor, an auditing firm, a law firm, a trading institution, an insurance company, a credit card issuer, a trading exchange, a government regulator, a law enforcement agency or other institution who may be involved with financial transactions. Similarly, financial investments can include investment and merchant banking, public and private financing, commodities and a securities trading, commercial and consumer lending, asset management, rating of corporations and securities, public and private equity investment, public and private fixed income investment, listing to companies on a securities exchange and bourse, employee screening, auditing of corporate or other entities, legal opinions relating to a corporate or other entity, or other business related transactions.

A log or other stored history can be created such that utilization of the system can mitigate adverse effects relating to a problematic account. Mitigation can be accomplished by demonstrating to regulatory bodies, shareholders, news media and other interested parties that corporate governance is being addressed through tangible risk management processes which include continual gathering of risk related information and application of the risk related information to transactions to assess a level of risk.

Information relating to financial, legal, regulatory and/or reputational risk is received as data into a computer system contained in the RMC system 106. The data can be related to a particular transaction, entity, person or other subject by keyword, fuzzy logic, artificial intelligence programs, full text, numerical value, financial value, coded entry or other well known or proprietary forms of data manipulation.

If desired, and in accordance with applicable privacy laws, the RMC system 106 or a subscriber 111 can apply an algorithm that weights risk related information in order to calculate a risk quotient or similar score or value rating indicating an amount of risk. The risk quotient can include, for example, a scaled numeric or alpha-numeric value.

If a transaction reaches or exceeds a risk quotient threshold, the RMC system 106 or subscriber institution 111 can respond with a predetermined action. Actions can include, for example, generating an alert, blocking acceptance of a transaction, creating a report, notifying a compliance department, or other appropriate response. In addition, the RMC system 106 or subscriber institution 111 can create a structured history relating to a transaction that can demonstrate due diligence and proper corporate governance. Reporting can be generated from the structured history.

In the case of an automated transaction, such as, for example, execution of an online transaction, a direct feed of information can be implemented from a system involved in the transaction to the RMC 106 or via questions presented to a transaction initiator by a programmable robot via a GUI. Questions can relate to a particular type of account, a particular type of client, types of investment, or other criteria. Other prompts or questions can aid a financial institution ascertain the identity of an account holder and an account's beneficial owner. If there is information indicating that a proposed transaction is related to an account that is beneficially owned by a high risk entity, the financial institution may not wish to perform the transaction if it is unable to determine the identity of the high risk entity and his or her relationship to the account holder.

The RMC system 106 can also receive open queries, such as, for example from subscriber personnel 112, wherein the query may or may not necessarily be associated with a particular transaction. The results of the query would contain information relating to an individual or circumstance associated with the query. The results may also provide historical data, world event information and other targeted information to facilitate a determination regarding an at risk entity's source of wealth or information related to particular funds involved with an account or transaction in consideration.

A query can be automatically generated from monitoring transactions being conducted by a subscriber institution 111. For example, an information system involved in a transaction can be electronically scanned for key words, entity names, geographic locales, or other pertinent data. A query can be formulated according to the pertinent data and run against a database maintained the RMC system 106. Other methods of query can include voice queries via a

telephone or other voice line, such as voice over internet, fax, electronic messaging, or other means of communication. Query can also include direct input into an RMC system 106, such as through a graphical user interface (GUI) with input areas or prompts.

Prompts proffered by the RMC system 106 can also depend from previous information received. Queries and information generally received, or received in response to targeted questions, can be input into the RMC system 106 from which it can be utilized for real time risk assessment and generation of a RMC risk quotient 108, quantified risk due diligence 109 and risk quotient aggregation 110.

An alert list containing names and/or terms of interest to a subscriber can be supplied to an RMC system 106 by a subscriber or other interested party. Each list can be customized and specific to a specific subscriber. The RMC system 106 can continually monitor data in its database via an alert query with key word, fuzzy logic or other search algorithms and transmit related informational data to the interested party. In this manner, ongoing diligence can be conducted. In the event that new information is uncovered by the alert query, the subscriber can be immediately notified, or notified according to a predetermined schedule. Appropriate action can be taken according to the information uncovered.

A risk assessment or risk quotient 108 can be made available by the RMS system 106 or a financial institution 111. In one embodiment, the risk quotient can be made assessed in real time. A real time assessment can allow financial institution 111 to provide a suggested action, which can be taken to address a particular risk quotient. A suggested action may include; for example, limiting the scope of a transaction entered into, discontinuing a transaction associated with high risk participants, notifying authorities, or other appropriate actions.

The RMC system 106 can quantify risk due diligence 109 by capturing and storing a record of information received, queries executed and actions taken relating to a transaction. Once quantified, the due diligence data can be utilized for presentation to regulatory bodies, shareholders, news media and/or other interested parties, to mitigate adverse effects relating to a problematic transaction. The data can demonstrate that corporate governance is being addressed through tangible risk management processes.

The RMC system 106 or the financial institution 111 can also aggregate risk quotient scores 108 to assess a level of risk being tolerated by the institution. Other calculations, such as, for example, the sum, mean, average, or other calculation can be made to further analyze risk at a financial institution. If desired, a rating can be applied to an institution according to the amount of risk tolerated by the institution, such as, for example, the average risk tolerated.

Referring now to Fig. 2, a network diagram illustrating one embodiment of the present invention is shown. An automated RMC system 106 can include a computerized RMC server 210 accessible via a direct connection 209 or via a distributed network 201 such as the Internet, or a private network. A subscriber 220-221, regulatory entity 226, information source 228, transaction personnel 224, or other party interested in RMC risk management, can use a computerized system or network access device 204-208 to receive, input, transmit or view information processed in the RMC server 210. In one instance, a network access device, such as a personal computer, can access the RMC Server 210. In another instance, a computer system, such as a backend system 211, can be linked to the RMC system 210 either through a direct linkage 209, such as a T1 line, or via a network 201. A protocol, such as the transmission control protocol internet protocol (TCP/IP) can be utilized to provide consistency and reliability.

If desired, a query request, alert list, or information can be sent to an operator of an RMC system 106 via traditional methods such that the operator can perform the query, implement the alert, or input the information. Traditional methods can include hardcopy, e-mail, fax, voice call or other well known means of communication.

A computerized system 211 or network access device 204-208 used to access the RMC system 106 can include a processor, memory and a user input device, such as a keyboard and/or mouse, and a user output device, such as a display screen and/or printer. The computerized system 211 or network access devices 204-208 can communicate with the RMC server 210 to access data stored at the RMC server 210. The computerized system 211 or network access device 204-208 may interact with the RMC server 210 as if the RMC server 210 was a single entity in the network 200. However, the RMC server 210 may include multiple processing and database sub-systems, such as cooperative or redundant processing and/or database servers, that can be geographically dispersed throughout the network 201. In some implementations, groups

of network access devices 204-208 may communicate with RMC server 210 through a local area network.

The RMC server 210 includes one or more databases 202 storing data relating to risk management. The RMC server 210 may interact with and/or gather data from an operator of a network access device 204-208, such as a subscriber 220-221, information source 228, transaction personnel 224, regulatory entity 226, or other person in control of the device 204-208. Data gathered from an operator may be structured according to risk criteria and utilized to calculate a RMC risk quotient 108.

In one embodiment, information received at the RMC server 210 can be identified as to an information source from which it has been received. Identification can be accomplished, for example, with a data tag indicating the source. Identification of a source of information received can be useful in order to refer back to the information source for additional related information, or to store proprietary information which can only be released to designated subscribers 220-221 or other designated entities, such as, for example, to comply with applicable privacy laws.

Typically, an operator or other user will access the RMC server 210 using client software executed at a network access device 204-208. The client software may include a generic hypertext markup language (HTML) browser, such as Netscape Navigator or Microsoft Internet Explorer, (a "WEB browser"). The client software may also be a proprietary browser, and/or other host access software. In some cases, an executable program, such as a Java™ program, may be downloaded from the RMC server 210 to the client computer 211 and executed at the client network access device 204-208 or computer 211 as part of the RMC system software. Other implementations include proprietary software installed from a computer readable medium, such as a CD ROM. The invention may therefore be implemented in digital electronic circuitry, computer hardware, firmware, software, or in combinations of the above. Apparatus of the invention may be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention may be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output.

Referring now to Fig. 3, steps taken to manage risk associated with a financial transaction with can include gathering or otherwise receiving information relating to risk entities and other risk variables 310. Informational data can be gathered from a subscriber or a source of electronic data such as an investigation firm, external database, messaging system, news feed, government agency, or other data provider. Typically, the RMC system 106 will receive data relating to a transactor, beneficiary or other associated party. Information can be received on an ongoing basis such that if new events occur in the world which affect the risk exposure of an transactor, an estimated risk value can be adjusted accordingly.

In addition to the types and sources of information listed previously that can provide indications of high risk, the financial institution or compliance entity can receive information that relates to requests to involve a financial institution that is not accustomed to foreign account activity; requests for secrecy or exceptions to Bank Secrecy Act requirements, routing through a secrecy jurisdiction, or missing wire transfer information; unusual and unexplained fund or transaction activity, such as fund flow through several jurisdictions or financial institutions, use of a government-owned bank, excessive funds or wire transfers, rapid increase or decrease of funds or asset value not attributable to the market value of investments, high value deposits or withdrawals, wires of the same amount of funds into and out of the account, and frequent zeroing of account balance; and large currency or bearer transactions, or structuring of transactions below reporting thresholds. Other information can include activities a transactor is involved in, associates of the transactor, governmental changes, attempting to open more than one account in the same time proximity, or other related events.

Sources of information can include, for example, publications issued by Treasury's Financial Crimes Enforcement Network ("FinCEN"), the State Department, the CIA, the General Accounting Office, Congress, the Financial Action Task Force ("FATF"), various international financial institutions (such as the World Bank and the International Monetary Fund), the United Nations, other government and non-government organizations, internet websites, news feeds, commercial databases, or other information sources.

The RMC server 210 can structure the information received according to defined RMC criteria 312. For example, information received can be associated with criteria including a

position held by the account holder or other transactor, the country in which the position is held, how long the position has been held, the strength of the position, the veracity of previous dealings with persons from that country, the propensity of people in similar positions to execute unlawful or unethical transactions, the type of transaction or other criteria.

Types of transactions can relate, for example to: an individual account, a public company domiciled in a G-7 country or Hong Kong, a public company not domiciled in a G-7 country or Hong Kong, a corporate account regulated by a G-7 agency or a corporate account regulated by a non G-7 government agency, a private company or partnership, a holding company, an intermediary managed account such as a money manager or hedge fund, a trust or foundation, or other type of legal entity.

The RMC server 210 can receive information 311and structure it according to predefined criteria or receive it in a pre-structured format. Receiving the information in a pre-structured format allows the RMC server 210 to proceed with storing and accessing the information without further refinement. Information that cannot be easily structured can also be received and archived in order to facilitate a manual qualitative evaluation.

The RMC system 106 can also receive an indication of whether the source of information wants the information tagged as originating from that source 312. Tagging can be useful for identifying which subscribers are free to receive which pieces of information and can also be useful to allow a subscriber to contact the source for further details related to the information. Tagging information with a source identifier 313 can be a default or done only on request and accomplished with a simple identifier associated with a module or record of information 313.

Once information is received, it can be structured and indexed according to RMC risk criteria 314, if desired. Accordingly, information can also be linked according to relations with other data in a database.

The RMC system 106 can receive a request for risk clearing 315 such as a query input to a network access device or a query formulated from monitoring key terms in a transaction. A report or other means of conveying the results of the query can then be generated 316. A risk quotient can also be generated 317 as well as a suggested action responsive to the risk quotient

318. Further details relating to generation of a risk quotient are listed below. Any results can be transmitted to the appropriate subscriber 319. The RMC system 106 can also receive a request from a subscriber for a link to the source of information transmitted to the subscriber 320 and provide such a link between the subscriber and the information source 320. The link can be an electronic interface, an e-mail address, a telephone or other contact information or means of communication. The RMS system 106 can also archive any information received, a risk quotient and a suggested action 321.

Referring now to Fig. 4, a flow chart illustrates steps that a subscriber or other user, such as a financial institution, can implement to manage risk associated with a transaction. The subscriber can receive information relating to an entity associated with a transaction 410. This information may be received during the normal course of business, such as when the participants to a transaction are ascertained. In one embodiment, software can scan a users computers responsible for transactions and glean pertinent information from the transactions taking place and transmit the information to the RMC system 106.

The user can access a RMC server 210 and identify to the RMC server 210 one or more entities, jurisdictions, or other risk variables involved in the transaction 411. Access can be accomplished by opening a dialogue with a RMC system. Typically, the dialogue would be opened by presenting a GUI to a network access device accessible by a person or an electronic feed that will enter information relating to the transactor. The GUI will be capable of accepting data input via a network access device. An example of a GUI would include a series of questions relating to a transaction. Alternatively, information can be received directly into fields of a database, such as from a commercial data source. Questions can be fielded during a transaction, or at any other opportunity to gather information.

In one embodiment, automated monitoring software can run in the background of a normal transaction program and screen data traversing an application. The screened data can be processed to determine key words wherein the key words can in turn be presented to the RMC server 210 as risk variables. The RMC server 210 will process the key words to identify entities or other risk variables. Monitoring software can also be installed to screen data traversing a network or communications link.

In one embodiment, a subscriber can calculate a risk quotient 413 by weighting the information received according to its importance in determining high risk activities, such as the likelihood of illegal or unethical dealings. Calculating a risk quotient can be accomplished by assigning a numerical value to each field of information, wherein the numerical value is representative of the risk associated with a particular piece of information. For example, it may be determined in one case that a government official from a G-7 country trading equities in a public company from a G-7 country poses minimal risk. Therefore this information from the first case is assigned a low numerical value, or even a negative numerical value. In a second case, an individual who appears on a list generated by the FATF and is attempting to transact in a corporate holding company may be viewed as a high risk. In another case, information conveying this high risk may be assigned a high numerical value. In addition, a weight can be assigned to a RMC risk category to which the information is assigned. Therefore a designated country may receive a higher weight than the position held, or vice versa. A Risk Quotient can be calculated by multiplying a weighted numerical value of the specific information times the category weighting.

For example, information received may indicate an transactor is a high ranking finance official from a G7 country. The ownership structure of a company the transactor wishes to transact is a public entity. A public entity may receive a numerical value of –5 because it is a relatively low risk ownership structure. In addition, this information may be included in a Company Profile category, wherein the Company Profile is assigned a category weighting of 3. Therefore, the net score for this ownership structure is –5 times 3 or –15. Similarly the transactor or associated account holder being a high ranking official from a G-7 country may also receive a low number such as 1. The RMC risk quotient for the transactor would be 1 times 3, or 3. All scores within the Company Profile can be summed to calculate a RMC risk quotient. In this case the RMC risk quotient is –15 + 3 which equals –12, indicating a low risk. Weighted risk scores from all associated categories can be summed to calculate a total Risk Quotient Score 108.

A suggested action can be generated that is responsive to the Risk Quotient 414. For example, in response to a high risk score a suggested action may be to not proceed with a

transaction, or even to notify an authority. In response to a low risk score, the financial institution may respond by completing transactions as usual. Intermediate scores may respond by suggesting that additional information be gathered, that transactions for this account be monitored, or other interim measures.

In addition to calculating a risk quotient 413, a user can also generate one or more suggested actions responsive to the risk quotient 414. A suggested action can include reasonable steps that can be taken by the financial institution or other user to address a risk that is associated with the transaction.

If a subscriber wishes to follow up by receiving more information or additional details regarding information, the subscriber can request a link from the RMC system 106 to an information source for particular information. For example, if the RMC system 106 has information in this database indicating that a particular person may have particular traits that cause the subscriber concern, the subscriber may wish to obtain additional information on that person. The RMC system 106 may have tagged the information when it was received with an identifier of the source of the information, for example an investigation firm. The subscriber can then request a link to the information source 415 and receive contact information to the investigation firm 416. This link can be utilized to pursue the additional information needed.

The user can also archive information relating to risk associated with a transaction as well as steps taken to address the risk 417. The process involved in utilizing the RMC system can be included in the archive as steps taken to diligently manage risk associated with a global transaction. In addition, reports can be generated to quantify the archived information and otherwise document diligent actions taken relating to risk management 418.

Referring now to Fig. 5, an exemplary GUI for displaying information related to RMC is illustrated 500. The GUI can include areas prompting for information, such as in the form of a key word or a question 501. Areas can also be included for an appropriate response 506. The area for an appropriate response 506 can, for example, receive text, allow a selection from choices proffered, or otherwise receive data into the RMC server 210. A programmable user interactive device, such as a checkbox, X field, yes/no filed or other device 503-505 can also be utilized to indicate an answer, or otherwise input information. Other programmable devices, such as programmable icons, hyperlinks, push buttons or other devices 502 can also be utilized

to execute a particular function. A category weighting area 507 can also be indicated on the GUI 500. Typically the weighting will be predetermined. However, if desired the weighting can be modified by a user such that a weighting value, such as a numerical value, will be utilized to calculate a risk quotient. The RMC GUI 500 can also include an area for displaying a quotient score relating to the transaction 508.

Referring now to Fig. 6, an exemplary GUI for presenting reports or suggested actions related to RMC is illustrated 600. The GUI for presenting reports 600 can include geographic areas of a user interface containing risk management procedures 601, including those procedures specifically followed in relation to a particular RMC or other suggested actions. Additional areas can include a list of electronic or hardcopy reports available concerning risk management efforts undertaken 602. Another area can include a list of risk quotients and./or calculations concerning a risk quotient, such as the average risk quotient for the financial institution, or the mean risk quotient 603. Still another area can contain information descriptive of a particular transactor or RMC 604.

A number of embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, network access devices 204-208 can comprise a personal computer executing an operating system such as Microsoft Windows™, Unix™, or Apple Mac OS™, as well as software applications, such as a JAVA program or a web browser. network access devices 204-208 can also be a terminal device, a palm-type computer, mobile WEB access device, a TV WEB browser or other device that can adhere to a point-to-point or network communication protocol such as the Internet protocol. Computers and network access devices can include a processor, RAM and/or ROM memory, a display capability, an input device and hard disk or other relatively permanent storage. Accordingly, other embodiments are within the scope of the following claims.